BLANKROME

300 Carnegie Center | Suite 220 |Princeton, NJ 08540
A Pennsylvania LLP | Stephen M. Orlofsky, New Jersey Administrative Partner
blankrome.com

Phone: *(609) 750-2646*
Fax: *(609) 897-7286*
Email: *stephen.orlofsky@blankrome.com*

April 20, 2022

BY E-MAIL

Arthur Armstrong, Esq.
Flaster Greenberg PC
1835 Market St.
Suite 1050
Philadelphia PA 19103
Arthur.armstrong@flastergreenberg.com

Eric Clendening, Esq.
Flaster Greenberg PC
One Tower Bridge
100 Front Street, Suite 100
Conshohocken PA 19428
eric.clendening@flastergreenberg.com

Adam Wolek, Esq.
Fox Rothschild LLP
321 N. Clark St.
Chicago IL 60654
awolek@foxrothschild.com

Melissa E. Scott, Esq.
Fox Rothschild LLP
747 Constitution Drive
Suite 100
Exton, PA 19341-0673
mscott@foxrothschild.com

Dominique J. Carroll, Esq.
Fox Rothschild LLP
Princeton Pike Corporate Center
Lawrenceville NJ 08648-2311
djcarroll@foxrothschild.com

Re: The HomeSource Corp. v. Retailer Web Services, LLC, et al., Civil Action No. 1:18-cv-11970

Dear Counsel:

I write in response to RWS's letter, dated April 13, 2022, seeking an extension of discovery to sixty days after I rule on the ongoing disputes over the mirror image of HomeSource's database, HomeSource's response to that letter dated April 18, 2022, and RWS's reply dated April 18, 2022. For the reasons explained below, I will allow for an extension to the close of discovery of sixty days after HomeSource provides the mirror image RWS for examination.

I. HomeSource's Web-Related Allegations

In its Second Amended Complaint, HomeSource has made numerous allegations about "various unlawful cyber activities" taken by RWS: (1) RWS published specific details about alleged security deficiencies in HomeSource's systems, and HomeSource subsequently suffered several DoS and DDoS attacks. Based on the this and the timing of those attacks "HomeSource believes that RWS was aware that the websites were going to be hacked . . . and at the very least, encouraged such hacks," (SAC at ¶¶ 50-73); (2) RWS accessed HomeSource's systems through unauthorized use of HomeSource's customer's log-in credentials, (SAC at ¶¶ 76-77); and (3) RWS ran spider and/or webcrawler software on HomeSource's websites which compromised the functionality of HomeSource's websites, (SAC at ¶¶ 79, 82). These alleged actions form the basis of several of HomeSource's claims:

- Count III – Tortious Interference with Prospective Economic Advantage (SAC at ¶¶ 101-02)
- Count IV – Tortious Interference with Contract (SAC at ¶¶ 110-11)
- Count V – Common Law and Federal Unfair Competition (SAC at ¶¶ 118-19, 121)
- Count VI – Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C) (SAC at ¶¶ 129-132)

II. Creation of the Mirror Image

Based on these allegations, at a hearing conducted on April 8, 2019, then-Magistrate Judge Williams instructed HomeSource to "create a mirror image of the data that it will search to determine whether RWS IP addresses are the source cause or relative to the alleged hacking that forms the basis of this case." (ECF 84 at 5:5-9.) This was followed by a written order that stated HomeSource:

> [S]hall immediately (if it has not already done so) create a Mirror Image of the data base it will use to compare RWS's IP addresses against for the purposes of determining whether any RWS IP address was connected to the alleged "hacking event." The Mirror Image shall have a hashvalue as it is beyond cavil that "hashing" guarantees the authenticity of the original data set.

(ECF 81.)

On October 7, 2019, the parties had another discovery conference with Judge Williams. In relevant part, the parties made arguments about the use of the mirror image. (Oct. 7, 2019 Tr. at

107:14-18, 107:23-108:5.) At that point, HomeSource had produced a summary of logs detailing visits to the websites in question, but had not provided RWS access to the database that produced the logs. (*Id.* at 108:24-109:10; 110:13-22; 112:18-25). The parties' primary disagreement was the proper scope of the searches to be conducted by RWS's expert on the mirror image: was RWS's expert required to only perform the same search that created the summary log produced by HomeSource in order to determine whether that log was accurate, or was the expert permitted to perform a search the best way they saw fit to determine the ultimate issue of whether RWS was responsible for web crawlers or other software on HomeSource's websites. After significant back and forth, Judge Williams stated that the role of RWS's expert was:

> [n]ot only to say the search that [HomeSource] ran was wrong, but that a proper search would have done this, and had a proper search been done, these are the results that would have been had. . . And so I've got to allow this expert to run the search that – that she believes is the proper search to determine whether or not RWS did whatever it did on your website.

Id. at 119:16-25. That conference was followed by an order which stated that:

> HomeSource shall make the "mirror image" of the database available to defendant's expert. The experts shall meet and confer and confirm the search undertaken by plaintiff's expert and the search protocol to be undertaken by defendant's expert. Defendant shall provide plaintiff with the search protocol. If there are objections to defendant's proposed search protocol, the parties shall present the issue to the Court.

ECF 129 at 4.

III. Disputes Regarding the Search of the Mirror Image

The parties have continued to dispute what methods can or cannot be used to examine the database and whether the information is relevant. In particular, RWS maintains that its expert is unable to develop search protocols without first examining the database, and HomeSource argued that the contents of the database is no longer relevant to the case, and that RWS was attempting to expand the use of the database beyond its intended purpose. In an attempt to resolve these issues, I ordered that RWS provide a list of each question it sought to answer through a search of the database, how that topic was relevant to the case, and what access and permissions its expert would need to develop a search protocol for those questions. ECF 287 at ¶ 1. I also provided for HomeSource to respond and object to any of those questions, and permitted RWS to respond to

those objections. *Id.* at ¶¶ 2-3.

In response to that order, on August 12, 2021 RWS submitted "Defendants' Searches of HomseSource's System per the Court's August 2, 2021 Order." This submission proposed seven questions it sought to answer through searching the mirror image:

1. "Did HomeSource create a forensically sound mirror image of its system? . . . . By assessing whether HomeSource preserved and created a forensically sound mirror image of the system, Dr. Bayuk will be able to assess whether (1) the mirror image can be properly authenticated, (2) the information and data relevant to HomeSource's allegations were properly preserved, (3) there was a properly preserved chain of custody, and (4) the data is reliable and ultimately can be used to support or rebut HomeSource's allegations. By accessing the mirror image, Dr. Bayuk will be also able to compare RWS's IP addresses against the mirror image for the purposes of determining if any RWS IP address was connected to the alleged 'hacking event.' Dr. Bayuk also require access to a mirror image archive of the system HomeSource claims was attacked by RWS. If such an attack occurred, that system would contain evidence of cyberattack. Bayuk Decl., at ¶ 37. If a corresponding hash value of that system at the time of the system archive was also archived, she 'could recompute the hash value from the mirror image.' Bayuk Decl., at ¶ 40."

2. "Did RWS attack or assist an attack on HomeSource on August 13, 2018? . . . Searching the mirror image would help assess whether there is any evidence on the mirror image to support HomeSource's allegations that (1) RWS was involved in the attacks, (2) the hacks originated from RWS, and (3) 'RWS ran a spider script against the three hacked websites,' as alleged."

3. "Did RWS attack HomeSource on or about September 26, 2019? . . . Searching HomeSource's system would help assess whether there is any evidence of cyberattacks on or about September 26, 2019 and if any evidence exists that those alleged attempts originated from RWS."

4. "In August and September 2018, did bots/spiders/web-crawlers 'continually send hundreds and thousands of requests to a single website in order to crash it, or at least, severely slow it down for other consumers trying to use the site,' SAC, at ¶ 61, and if so, did RWS's visits markedly contribute to slowing down HomeSource's computer systems? . . . Searching the mirror image would help assess whether there is any evidence on the mirror image to support HomeSource's allegations that (1) someone utilized bots and/or programs targeting HomeSource's customers' websites in August and September 2018, (2) the alleged bots and/or programs caused the customers' websites to crash, (3) the website visits and searches originated from Scottsdale, Arizona, (4) the website visitors and searches originated from RWS, and (5) the visits and searches originating from RWS were sufficient to substantially interfere with and/or crash the customers'

websites."

5. "Did RWS obtain HomeSource's proprietary information without authorization? . . . Searching the mirror image would help assess whether there is any evidence on the mirror image to support HomeSource's allegations that (1) RWS logged into HomeSource's websites without authorization, and (2) RWS obtained proprietary information."

6. If HomeSource uses information from its database to support that it entered into contracts with alleged lost customers, the database will need to be searched to verify whether HomeSource indeed did have contracts with its alleged lost customers and the support HomeSource has for those contracts. . . . As explained in Dr. Bayuk's Declaration, if HomeSource produces additional information evidencing 'lost customers' that is on its systems, then RWS will need to analyze HomeSource's system to assess and verify the 'click-through' agreements are indeed agreements and are indeed for HomeSource's 'lost customers,' and to verify the terms of those agreements. Bayuk Decl., at ¶ 95."

7. "Did a 'security hole and vulnerability' exist in 'HomeSource's systems' in July 2018? . . . Searching HomeSource's system would help assess whether there is any evidence of security holes and/or vulnerabilities that existed in HomeSource's systems in 2018."

On August 23, 2021, HomeSource submitted its objections to these queries. As an overarching objection, HomeSource noted that the mirror image contained very narrow, specific information. It stated the mirror image was of a "Log Server" and that "HomeSource created the Log Server to provide logs of all the IP requests that hit HomeSource's system during cyber and/or DDoS attacks that occurred between August and September 2018, and on September 26, 2019. No other content, (e.g., contract information, customer names, and financial data) is contained in the Log Server." HomeSource Objections at 3. As a result, they note that "queries 4 through 7 seek information that is simply not part of the mirror image database." *Id.* at 1. They further object to queries 2-7 on the grounds that, because the Log Server was never meant to contain information outside of those specific parameters an absence of results from RWS's proposed search "does not constitute evidence that the information doesn't exist." *Id.* at 3, 6, 7, 8; *see also id.* at 4, 5 (incorporating objections). Additionally, in regards to Query 1, HomeSource objected that RWS's proposed protocol to verify its hash value – and by extension the integrity of the mirror image – would in fact alter the hash value. Instead, they argue that the only way the Log Server can be validated is "an examination of the storage record with AWS." *Id.* at 2.

On September 2, 2021 RWS responded to HomeSource's objections. RWS argued that HomeSource's objections regarding what conclusions its experts would be permitted to draw based

on the lack of information in the mirror image were a premature *Daubert* motion, and that if the relevant information it sought was not located in the mirror image, HomeSource had the obligation to produce that information, or inform RWS of its location so that it could be examined. RWS also maintains that the search protocol proposed to authenticate the mirror image is industry standard, and questions why the mirror image was created in a way that it cannot be viewed or verified.

IV. The Mirror Image Remains Relevant to the Litigation

Factual issues regarding the alleged DoS and DDoS attacks on HomeSource, unauthorized access to HomeSource's systems, and use of webcrawlers or similar software on HomeSource websites are all still relevant to this case, despite the severance of claims against the John Doe defendants. Although HomeSource contends the CFAA claim against RWA is *not* related to the DDoS and DoS attacks, and that the mirror image only contains information related to those attacks, that does not make the mirror image irrelevant. First, aside from the CFAA claim against RWS, HomeSource also alleges that HomeSource was "aware that the websites were going to be hacked, before those websites were actually hacked on August 13, and at the very least encouraged such hacks with RWS's internet post." SAC at ¶ 70. Further, HomeSource cited the "various unlawful cyber activities set forth above" as a basis for several of its non-CFAA claims: Tortious Interference with Prospective Economic Advantage (SAC at ¶ 101), Tortious Interference with Contract (SAC at ¶ 110), and Unfair Competition (SAC at ¶ 118). This can only be read to include RWS's encouragement or passive involvement with the DoS and DDoS attacks, which then in turn requires proving such attacks occurred. This makes the mirror image, which logged the visits to the website during those attacks, relevant.

Aside from the hacking events, the mirror image could also be relevant to questions regarding the "spiders" that HomeSource alleges were deployed on HomeSource websites and "slow[ed] the functionality of the websites." SAC at ¶¶ 79-82. Because the Log Server would contain visits to the website over a period of time, that may contain evidence of spiders visiting the website, and the relative volume of that activity compared to overall visitation to the site, making it more or less likely that those spiders slowed the functionality of the website. This is also why examination of the mirror image is not duplicative of "the list of IP addresses from the bots/spiders/web-crawlers that originated from RWS and hit its sites in August and September 2018" -- aside from the possible issues of authentication and best evidence that this list may invoke.

V. Resolution of the Outstanding Dispute

To resolve the remaining disputes surrounding the mirror image database, the parties

BLANKROME

should have one final meet and confer in the next ten days to attempt to resolve the remaining issues. If the parties are unable to come to an agreement, I will consider appointing a neutral expert to oversee the examination of the mirror image, the cost of which would be split by the parties, in light of the highly technical issues regarding the validation of the mirror image through the hash value, and allegations that reviewing the mirror image could irreparably change that value. *See* Fed. R. Evid. 706 (permitting courts to *sua sponte* issue an order to show cause for the appointment of an expert witness it selects).

To attempt to make this meet and confer more fruitful than those in the past, I will highlight several considerations for the parties. Dr. Bayuk's examination of the mirror image will allow her to draw conclusions regarding only that: what is on the mirror image. If Dr. Bayuk draws any conclusions beyond that, they can be subject to a *Daubert* motion. That being said, although the mirror image may not contain all evidence of the "various unlawful cyber activities" RWS is accused of, any other sources of that evidence should have already been produced or otherwise disclosed. If HomeSource later attempts to support its claims, through an expert or otherwise, relying on web logs or databases other than the information contained on the mirror image, it may be subject to motions in limine and exclusion, for violation of its ongoing duty to preserve and disclose relevant information. Therefore, if HomeSource intends to rely on other databases, servers, or sources of technical information and metadata to prove its claims, it should disclose that at the meet and confer and provide a plan to give RWS access to examine those materials, given the impending close of fact discovery. Finally, although HomeSource is correct that it has no obligation to withdraw any claim or allegation, if it does, that may make this discovery irrelevant.

I intend to file this letter via ECF. If either party believes any information in the letter should be redacted prior to filing please provide me with proposed redactions by Friday April 29, 2022.

Very truly yours,

/s/ Stephen M. Orlofsky

STEPHEN M. ORLOFSKY
Special Master